Proposed changes and additions to DCID 1/19
to clarify SCIF accreditation procedures and to establish
procedures for joint use of SCIFs

(para. 13, last sentence)

"Accrediting officials shall maintain records on each SCIF they accredit. These records shall include a physical security profile on each SCIF, all changes to that profile, all waivers of standards, the accreditation and any agreements covering joint use of the SCIF. These records also shall include documentation on inspections and surveys conducted initially and thereafter to establish and maintain security integrity of each SCIF. These records shall be available for inspection by the DCI or his designee. (U)

(new para. 14, renumbering existing 14 and following)

14. Joint Use of SCIFs. Joint use of industrial contractor SCIFs is encouraged to make efficient use of resources and reduce costs to the US Government. Each instance of joint use of a SCIF shall be covered by a memorandum of agreement (MOA) among the parties involved. As may be mutually agreed, one of the Intelligence Community agencies holding a contract with the industrial contractor involved will be designated the Cognizant Security Authority (CSA) for purposes of the MOA. The CSA, the other agencies wanting to share the same contractor SCIF, and the industrial contractor shall prepare an MOA specifying who is responsible for what security measures and who is to provide what security equipment or services. The form of the MOA is left to the discretion of the parties involved, except that it must be in writing. (Electrical messages are not acceptable for the agreement. In an emergency, however, joint use may be entered into on the basis of electrical messages, but must promptly be confirmed by a written MOA.) Signatories must be

responsible officials of the CSA, other involved agencies and the contractor. MOAs shall be classified (and compartmented) whenever they cover matters requiring security protection and control. A signatory agency which wants the contractor to make any substantive changes in procedures or physical characteristics of the jointly used SCIF shall obtain the prior concurrence of the CSA. The CSA is responsible for notifying other signatories of the MOA who would be substantively affected by the proposed change(s). User agencies must notify the CSA in advance of their plans to withdraw from joint usage. Joint use of computer systems at contractor facilities is covered by DCID 1/16. A separate MOA is required for such use. (C)

Proposed Additions to DCID 1/16

(add the following new paragraphs to Chapter I of the Computer Security Manual)

Accreditation. All automated systems and networks which process classified intelligence or counterintelligence must be accredited before being put in service. Accreditation authorities and duties are specified in Chapters II and III of this manual for systems and networks respectively. The accreditation statement must be supported by complete documentation which fully describes the technical assessments of each automated system or network; its vulnerabilities, risks to it and countermeasures to them; and the results of security tests and analyses which have been performed on it. Accreditations shall be updated whenever substantive procedural, or physical changes are made to a system or network. Accreditation files shall be available for inspection by the DCI or his designee. (U)

Joint Usage. When more than one Intelligence Community agency uses an automated system or network, or when systems or networks from different agencies are concatenated, a memorandum of agreement (MOA) shall be executed to specify who is responsible for what security measures and who is to provide what security equipment or services. In addition, the concatenated systems or networks must be accredited as a unit. As may be mutually agreed, one of the agencies involved will be designated the Principal Accreditation Authority (when a single system or network is shared) or the Joint Accreditation Authority (when systems or networks are concatenated). The MOA must identify the level(s) of classification (and compartmentation) of data to be processed, and any operational restrictions placed on the system(s) or network(s). MOAs shall be signed by the Princiapal Accreditation Authority, or Joint Accreditation Authority as applicable, the accreditation authority(ies) for

other systems or networks which are concatenated, responsible officials or user agencies, and, if applicable, representatives of industrial contractors participating in the system of network. MOAs shall be updated whenever substantive procedural or physical reconfiguration changes are made to the system(s) or network(s) involved. The form of the MOA is left to the discretion of the parties involved, except that it must be in writing. (Electrical messages may be used initially when circumstances dictate, but must be followed up by signed hard copy documentation.) MOAs shall be classified (and compartmented) as appropriate to the sensitivity of the information they contain. (C)